Wiley Handbooks in Criminology and Criminal Justice

The Handbook of The Criminology of Terrorism

Edited by Gary LaFree and Joshua D. Freilich

31

The Ten Commandments for Effective Counterterrorism

Simon Perry, David Weisburd, and Badi Hasisi

The terrorist threat has significantly impacted life in Western democracies. Thus, law enforcement and intelligence and security agencies need to collaborate to protect citizens in democratic societies. Terrorists strive to create fear and anxiety and diminish the resilience of society. Their goal is to destabilize the social order by increasing the frequency and intensity of attacks and inflicting mass casualties. Therefore, effective counterterrorism is geared toward helping the general public maintain their daily routines and personal sense of security by deterring, uncovering, foiling, and defeating attacks; ensuring efficient first response; and facilitating recovery from these attacks (Howard, 2004; Weisburd et al., 2009; Perry, 2014).

Even though counterterrorism has become a major task for law enforcement, there are only a handful of counterterrorism models that demonstrate effective strategies, tactics, and best practices for policing terror. What is more, not much is known about how these models can be systematically evaluated and quantified for their effectiveness (Lum et al., 2006; Weisburd et al., 2009; Perry, 2014). The lack of evidence-based counterterrorism models and of systematically evaluated strategic and tactical measures is a result of two factors. First, law enforcement intelligence and security agencies are not enthusiastic about collaborating with researchers because they fear this could expose and compromise their counterterrorism methods, tools, sources, and tactics. Second, this type of research runs into difficulties in operationalizing success. The determination of cause and effect is complex because of other historical variables, which make the creation of a control situation complex (Perry, 2014).

The development of evidence-based practices for effective police tactics for responding to terrorism has begun to receive attention from criminologists. According to Clarke and Cornish (2001), crime is primarily an outcome of a *process* wherein the individual assesses *opportunities*, evaluating the expected benefits of a behavior against the probable costs, in the circumstances of a particular time and place. Therefore, Weisburd and Waring (2001) elaborate on Felson and Clarke's 1998 approach, and argue that effective crime prevention implies decreasing the *opportunities* that specific situations grant and that encourage the commission of a crime. Clarke and Newman (2006) claim that the behaviors that encompass

The Handbook of the Criminology of Terrorism, First Edition. Edited by Gary LaFree and Joshua D. Freilich.

terrorism (even suicide terrorism) are similar to behaviors of conventional "ordinary" criminals. They conclude that terrorism is a form of crime, and that terrorists are criminals. Perry and Hasisi (2015) also argue that the terrorist's rational choice cost-effect decision-making is similar to non-terrorist offenders. For that reason, they claim that practical counterterrorism should mostly deploy proven situational crime prevention techniques, which have effectively prevented regular crime.

This chapter introduces and reviews "Ten Commandments" for best counterterrorism practices. These practices encompass proven strategies, tactics, and practices from the field of policing terrorism.

First Commandment—Reduce the Opportunities for Terrorists to Attack

Terrorism, like any other criminal behavior, is a result of two preexisting conditions: *motivation* to perform the terrorist activity, and *opportunity* to carry it out in certain circumstances (Clarke & Newman, 2006). As a result, prevention may be carried out by either neutralizing *terrorist motivations* or reducing *terrorist opportunities*, or both (Perry, 2014). Terrorism is viewed by the "conciliatory model" as a political problem that should be prevented by resolving the motivation to commit terrorist activity. Therefore, a political solution should be provided by policymakers, brokers, and diplomats to address the root causes of terrorism (Greene & Herzog, 2009). Conversely, Clarke and Newman (2006) maintain that counterterrorism "must not rely on changing the heart and minds of terrorists. The motivation for terrorism results from long-term social, cultural and psychological pressures, which are difficult to alter" (Clarke & Newman, 2006:11). They claim that it is easier to reduce terrorist *opportunities* than to moderate terrorist *motivation*, and that easy opportunities encourage terrorists to attack. Consequently, the most effective method for preventing terrorism is to implement strategies that remove the opportunities to execute terror strikes.

Neutralizing terrorist motivations is not a primary mission for law enforcement. Moreover, it appears less effective in preventing terrorism than by reducing opportunities. Thus, most counterterrorism strategies focus on trying to decrease *opportunities* rather than reduce *motivations*.

According to Clarke and Newman (2006, p. 9), there are four "pillars of terrorism opportunity": targets, weapons, tools, and facilitating conditions. Effective counterterrorism should therefore reduce terrorists' capabilities and opportunities to reach and harm targets or to produce or acquire weapons and tools, and minimize the facilitating conditions to perform an attack.

Second Commandment—Reduce Opportunities Proactively and Responsively, Combining Offensive and Defensive Measures

Opportunities can be reduced defensively and/or proactively. In fact, law enforcement routinely uses both reactive and proactive approaches. In the reactive response, law enforcement agents respond after the fact to a crime or a terrorist act. Police reactions include collecting evidence, gathering intelligence, identifying perpetrators, and arresting suspects. This reactive approach is a defensive method that could at best prevent a strike that has

been instigated, or minimize the damage of the attack. In addition, the defensive model aspires to protect potential vulnerable victims and targets from further aggression through "target hardening" (Clarke & Newman, 2006; Weisburd et al., 2009), and seeks to restore order and calmness after attacks have been committed.

The proactive model strives to thwart the crime/terror attack prior to its instigation. This model has been practiced by law enforcement for decades to deal with terrorism. It is based on intelligence gathering and analysis, and operational execution. Typically, law enforcement intelligence identifies potential criminals/terrorists, collects incriminating intelligence and evidence, and foils the crimes/attacks before they occur, by arresting the perpetrators. The core of this scheme, which has been classified as "high policing" (Bayley & Weisburd, 2009; Brodeur & Dupeyron, 1993), is the employment of covert intelligence gathering, surveillance, and operational prevention tools. Proactive prevention seeks to harm terrorist organizations and individuals physically, psychologically, and financially, to strike at their operational capabilities, infrastructures, morale, and motivation. These proactive measures are intended to deter, disrupt, and prevent terrorist activities (Weisburd et al., 2009; Hasisi et al., 2009; Perry, 2014).

The proactive approach also drives terrorists into a defensive mode, where they spend a great deal of time and resources concealing their activity, thus limiting their ability to carry out attacks (Perry, 2014). In the modern era of globalization, terrorist groups tend to be elusive targets, taking advantage of open democratic societies and utilizing advanced communication technologies to evade traditional security agencies' surveillance. Some of these stateless terrorist groups are aided by supporting states and territorial terrorist entities. As a result of this continually changing character of terrorism, the proactive strategy is becoming more complex (Hasisi et al., 2009).

Unfortunately, it is impractical to entirely prevent all terrorist attacks; therefore, it is good to have in place an effective defensive reactive approach alongside the proactive routine. This joint approach is complementary rather than contradictory. A combination of both methodologies could prevent or at least minimize terrorist opportunities to attack, halt in-progress attacks, reduce the amount of the casualties and damage, as well as restore order and a sense of safety. Such a comprehensive counterterrorism model allows the public to maintain their everyday routines and preserve their morale and resilience.

In the past, it was common for local law enforcement officers in the United States to view themselves primarily as "first responders." This is changing, and officers now also see themselves as "first preventers" of terrorism. Connors and Pellegrini (2005) claim that, if local officials and police in the United States want to prevent or recover from future terrorist attacks, they ought to take the lead on counterterrorism, and not depend upon federal agencies located hundreds of miles away.

Weisburd and Braga (2006) note that evidence-based studies have found that proactive policing tactics have prevented crime. The New York City police department has adopted this successful concept of "prevention" and adapted it for the war on terror (Bratton & Kelling, 2006).

According to Innes (2006), proactive, intelligence-led policing was initiated in the United Kingdom as early as the 1990s. The police have improved their effectiveness by identifying suspicious people and vulnerable places, and then focusing on crime prevention. Since the police have limited resources, and live informants ("HUMINT"—HUMan INTelligence) are difficult to develop, they often rely upon networks of community intelligence contacts to scrutinize potentially dangerous individuals. Proficient units were created to develop and maintain this "community intelligence feed" that would serve both anti-criminal and

anti-terrorist purposes. This transformation reflects a more proactive mode of operation based on the principles of risk management (Perry, 2014).

The Israeli model for policing terrorism has a long history of combating terrorism and is efficient and professional in its counterterrorism approach (Weisburd et al., 2009; Perry, 2014). The Israeli security apparatus combines proactive offensive and reactive defensive methodologies. It is executed in three circles of activity: (a) *sources of terrorism*—proactive early prevention, interdiction, and treatment of the sources of terrorism to thwart terrorist attacks before they are instigated; (b) *the attack route*—response activities once an attack has been launched, to foil terrorist attacks before they reach the target; and (c) *the terror targets*—defending and "hardening" potential targets before any attack, and response activities at the scene during and after an attack.

The Israeli counterterrorism model emphasizes proactive actions, because it focuses on detaining terrorists, reducing the frequency and severity of attacks, and thus resulting in fewer casualties. This proactive mode has a superior counterterrorism outcome, preventing terrorists from achieving their objectives, and allowing the general public to preserve their everyday routines (Perry, 2014).

Third Commandment—Execute Proactive Offense Based on Quality, Available and Timely Intelligence, and Operational Capabilities

The proactive offensive mode is fundamental for preventing attacks before they are instigated, and therefore is the most effective counterterrorism strategy. By developing quality intelligence and instituting operational capabilities, it enables police to identify and respond to terrorist threats before they actualize, and to uproot terrorists and their infrastructure (Weisburd et al., 2009; Perry, 2014). This proactive scheme is based on two imperative capacities: producing quality intelligence and creating operational capability. *Quality intelligence* is the capacity to collect, in real time, reliable information about the terrorists' capabilities, intentions, and specific plans, analyzing and disseminating this intelligence for use in police operations. Quality intelligence seizes the element of surprise, which is the key advantage for a terrorist attack, placing the element of surprise in the hands of law enforcement.

The production of quality intelligence is a circular process that is continuously set to reveal a reliable depiction of the threats. The intelligence analyst defines (based on the initial information) the information gaps—that is, the missing information needed to generate a reliable intelligence picture. This *intelligence picture* is composed of all the information about matters that are significantly linked to the various threats, which are called "topics of interest," and all the information about individuals who are coupled significantly and create the threat, who are called "targets."

For the purpose of revealing the missing information and closing the "intelligence gaps," an intelligence plan is prepared for collecting and exposing the potential threats. The plan comprises three levels of information gathering: the abovementioned "topics of interest" and "targets," as well as the territorial coverage, which is the entire information about a specific area (neighborhood or town), including who is doing what, when, and where, and who knows about it. At the initial phase, potential sources of information are identified to collect information on all three levels. At the next step, a "recruitment plan" is prepared, which includes the recruitment methodology and the scheme of running the various live informants ("HUMINT") and technical sources (called "SIGINT"—signals intelligence,

including wiretaps and surveillance activities). Other sources of information include investigations and debriefings, archives, and databases; public open information such as the news media and the Internet; and fellow agencies from the same country or international (Perry, 2014).

All information collected from various sources flows to the "nerve center"—where analysts prepare and present an integrated "intelligence picture." Their job is an unending process: they direct the collection of intelligence according to the requirements of the management directive guidelines; they support the development of "HUMINT" sources; they develop and deploy intelligence capabilities and tools; they handle the Intelligence Database; and they assist in the preparation of an operational activity. Police intelligence generally deals with criminal organizations that are small active groups from within the civilian setting, where as HUMINT sources are considered effective for penetrating regular criminal organizations whose structure and character resemble terrorist groups (Perliger et al., 2009).

The mere gathering of quality and timely counterterrorism intelligence without the capacity to seize control of the target and/or prevent the attack is insufficient. The task of capturing the target and/or preventing the attack is executed by special operations units with the skills to enter the scene where terrorist actions are being planned and prepared. These special operations units have a dual mission: First, to utilize the intelligence to foil the attacks before they are launched; and second, to surprise and threaten the terrorists' own sense of security, keeping them busy and on the run. Such units should be able to conduct undercover operations in which they reach and arrest their target without being detected. The police should deploy specialized elite counterterrorism units, trained to handle very specific terrorist situations, such as releasing hostages and carrying out special operations using small disciplined teams highly trained in commando-style military operations (Perry, 2014).

Bratton and Kelling (2006) claim that the police should organize special training programs to proactively attack terrorism. Police departments from all over the world are exchanging information with other countries to confront this global threat. Israel, for example, has welcomed police forces from all over the United States for training and exchange visits.

Fourth Commandment—Implement "Target Hardening" Based on a Risk Analysis for Vulnerabilities

Police and security resources are limited, while the number of potential targets is endless. Yet, not all targets are similarly attractive for terrorists. Therefore, the police need to conduct an efficient defensive effort, using vulnerability and risk analysis based on intelligence to build an effective protection plan. Vulnerability and risk assessment must then drive operational responses to create a truly effective policing apparatus against terrorism (Connors & Pellegrini, 2005). Intelligence and risk assessment allows security forces to protect, in advance, potential targets that may be selected by terrorists. The plan needs to prioritize the allocation of defensive tools to harden the more vulnerable potential targets. Davis et al. (2004) claim that, before 9/11, only a quarter of the police departments in the United States conducted risk assessments, compared to three-quarters that carried out such analyses after 9/11. Private security firms are the police's main collaborators in "target hardening."

The police force needs to train, and to provide necessary information and supervision to facilitate the private security firms' ability to better protect their clients' facilities. In Israel,

all public facilities, such as office buildings, malls, shopping areas, restaurants, and hospitals, have private security operatives who check customers entering the facility and conduct other security-related activities. The police, before approving the business licenses for any facility to operate, examine the business' facilities and their security procedures. The police carry out periodic security exercises at active businesses, in which facilities that do not hold to the security standards set by the police may be shut down through court orders (Weisburd et al., 2009; Perry, 2014).

Since it is not realistic to attack-proof all possible targets, the protection plan should aspire to minimize the number of victims and damage in case a terrorist attack is not thwarted. For example, the private security, guided by the police, should prevent terrorists from accessing indoor public facilities. The principle here is that an explosion that strikes within a closed environment (especially if crowded) will result in more destruction than if the same explosion occurred outdoors, hopefully away from the large crowd.

The security method of "target hardening" is modular, entailing four security elements whose purpose is to deter and minimize situational opportunities among any terrorist potential attackers, as well as to effectively neutralize any aggressor, and to prevent the loss of human lives, injuries, or property damage. These four security elements are:

1. Armed security first-response personnel that should: protect the population by facilitating a self-defense first response in the time of need; strengthen the sense of security; and deter any threats to safety. This security element of protection is composed of different levels of intensity.
2. Improvement of facility defense by means of physical and organizational security "target hardening," which includes elements such as gates, security fences, secured entrance gates for vehicles, emergency one-way exit gates, public announcement systems (PA systems), CCTV systems, communication and alarm systems, public response systems, emergency centers, etc. Target hardening by installing security measures lessens the target's vulnerability and its attractiveness to potential perpetrators. Assessing the vulnerabilities of the inherent features and addressing them are important elements in the overall level of safety and protection from attempted attacks.
3. External reinforcement conducted by the local police force (before, during, or after an attack incident).
4. Preparedness through training and drills.

An other important element of target hardening is educating the public and improving routine security preparedness, which will be discussed in the Tenth Commandment (Educate, Communicate, and Update the Public before, during, and after a Terrorist Event).

Fifth Commandment—Constantly Create a Hostile Operating Environment for Terrorists through Bottleneck Passages that Generate Intelligence Footprints

The "broken windows" theory, according to Bratton and Kelling (2006), generates a hostile setting for potential criminals, creating the uncomfortable sentiment that they are the ones threatened. Similarly, law enforcement's intelligence and security apparatus should produce a hostile environment for terrorists. That should be done primarily through potential terrorist support structures, constantly changing the terrorists' operating environment by

establishing "bottleneck passages." Bottleneck passages, such as obstacles and barriers, force terrorists to take counteractions, involving other co-conspirators. The participation of other co-conspirators forces the usage of extra communication channels, leaving "intelligence footprints," thus increasing the prospects for intelligence collection by both human and signal technical channels. Ongoing intelligence and operational pressure will result in terrorists feeling unable to rely on partners; it will prevent them from remaining at a given place for more than a short time, causing them to sleep every night at a different location, and putting terrorists constantly on the run in a distressing self-preservation mode. By keeping terrorists busy and on the run, it is possible to uproot them and their infrastructure, pushing them into a defensive and ineffective mode. As a result, they will need to spend more time on self-preservation and have less time, resources, and capabilities to plan and carry out terrorist attacks. The creation of a hostile environment for the terrorists will also take away the element of surprise from the terrorists and put it in the hands of the law enforcement, intelligence, and security apparatus.

Sixth Commandment—Conducting Drills in Order to Train Security Forces in Effective Methods of Delaying Attacks That have Already been Launched

Once a terrorist attack has been launched and set in motion, security forces employ intelligence both for proactive offensive thwarting operations and for responsive defense measures (Perliger et al., 2009). In a response to attacks that are not thwarted by the offensive–proactive activity, terrorists should be stopped once they are on their way to the targets. To foil launched attacks, there is a sequence of workable procedures to delay the terrorist's movement, once an attacker is en route to the target. The series of possible tactics includes setting up roadblocks, generating traffic jams, and closing certain public facilities or streets. There are two main purposes for generating such obstacles: The first is to slow down the terrorist to delay the attack. This provides the police with more time to bring special operations units to engage with the terrorist on course, and to simultaneously organize better defense for the potential terrorist target(s). The second purpose of the obstacles is to compel the terrorist to establish additional communication channels that increase the prospects for enhanced "HUMINT" and "SIGINT" intelligence gathering. The enriched intelligence and better police deployment allow special operations units to engage with the terroristen route and increase the probability for interdiction before the attack takes place.

As soon as there is a specific threat that terrorists have penetrated through the security, the police should consider using the media to inform the public to stay away from crowded locations.

Seventh Commandment—Secure, Evacuate, Restore Order, and Collect Evidence and Intelligence at an Attack Scene—Effectively and Rapidly

As first responders, obviously the police are expected to respond both during and after a terrorist attack, and to do so effectively to manage the crisis at targeted sites. The Israel National Police (INP), which has immense practice in managing numerous terror attack scenes, has developed effective procedures.

A basic principle of managing an attack scene is that there is a clear division of authority. Through the whole process, the highest territorial police commander present at the scene is in charge and answerable for all activities that occur until he or she has been released by a higher commanding officer, or when the scene is cleared. The overall responsibility is never divided, and it is always transparent. Throughout the process, all other organizations at the attack scene are subordinated to the police commander, including the medics, the firefighters, and even the employees of the local city council who will later clean the area (Weisburd et al., 2009; Perry, 2014).

The first assignment is to secure the scene from secondary explosive devices or additional terrorists. This procedure addresses a terrorist attack method by which they target the first responders, policemen, and the medics, who are first on the scene of an attack. Consequently, the first allowed on the scene are the bomb-squad technicians, who isolate and search the scene. Only those medics who treat and evacuate the most critically injured are allowed on the scene at this phase, along with the bomb-squad technicians. The remaining injured individuals are cared for and evacuated only after the scene has been secured. Deceased persons identification forensic personnel (a unit within a special civil unit) follow, to identify the dead and evacuate the bodies. The bomb squad laboratory collects remains to identify the type of explosive device or weapons used, for the purpose of linking it to a specific terrorist organization and/or bomb maker. At the same time, the forensic field unit collects evidence with the criminal investigators. Simultaneously the traffic and patrol officers handle the outer ring of the attack scene: they place road blocks isolating the attack scene, guide traffic, clear the way for ambulances, search for any co-conspirators who might have assisted the attacker and are trying to get away, and control the crowds. Intelligence units collect information that may assist in identifying the source of the explosives and the people responsible (Weisburd et al., 2009; Perry, 2014).

As mentioned, to defeat the goals of terrorism, the main object of police counterterrorism strategies is to strengthen the population's resilience, enabling them to continue with their daily routines. It is expected that a swift clearing of the terrorist scene reduces the psychological consequence of the attack. Hence, timing is essential, for psychological reasons. Punctual treatment of the scene is also important for forensic reasons, to collect evidence before the scene is contaminated. In the Israeli model, all of these activities of working on clearing and normalizing a terrorist scene are expected to be completed in a maximum of 4 hours.

Eighth Commandment—Deploy, Equip, and Train Fast Response Teams

An effective response to terrorism requires the ability to organize and respond quickly and proficiently to prevent or at least reduce the damage of a terrorist attack. Police officers must thus be trained and equipped to confront the terrorism threat. Kelling and Bratton (2006) maintain that counterterrorism has to be woven into the working procedures and practices of every police department, so that it becomes part of the daily thoughts of officers on the street.

All police officers, including those whose central task in the police force is not counterterrorism, ought to go through basic counterterrorism training. This training should drill officers for an unanticipated encounter with a terrorist episode. It should focus on imparting first-response expertise (such as isolating the location of a terrorist attack effectively). At a higher level of response, the police should form and train fast response teams that

would defuse terrorist events and terminate them as soon as possible. The objective of such teams is to prepare for fast intervention to minimize the harm, and to contain the event until the attack is resolved or the special counterterrorism unit takes over. Response time is crucial in containing a terrorist attack; thus, the fast response teams ought to receive adequate training (such as in urban warfare), applicable drills, equipment, and suitable transportation, such as motorcycles (Weisburd et al., 2009; Perry, 2014).

Ninth Commandment—Clearly Define the Division of Authority and Responsibility, and Practice Crucial Procedures and Inter/intra-agency Cooperation and Partnerships

A number of democratic countries have a highly centralized police organization at the national level, with a distinct purpose and responsibility related to crime, terrorism, and public order. Nevertheless, even in such circumstances, the police force has partners in counterterrorism. Additionally, each police force is composed of various units, so that harmonized cooperation does not always come naturally. This is especially true in the chaotic reality of a terrorist attack; therefore, it is crucial to have an unmistakable division of authority that unequivocally designates the one person in charge at a certain time and place, bearing ultimate responsibility. Vagueness about who is managing the incident leads to confusion and failure that will end with unnecessary victims and destruction.

Israel, for example, has a national hierarchical and centralized police force (Israel National Police, INP), with special centralized operational counterterrorism units. The internal security intelligence gathering in Israel is also centralized, which further contributes to the efficiency of deterring, detecting, identifying, and thwarting processes of potential terrorist attacks (Greene & Herzog, 2009). There is personal and constant formal and informal cooperation between the police and the Internal Security Agency (ISA) (Weisburd et al., 2009; Perry, 2014). This intimate partnership between the INP, which has overall responsibility for internal security, and the ISA, which is the main initiator of counterterrorism intelligence, was not a minor accomplishment. It took immense effort at all operational and command levels to create this trusting relationship between the INP and the ISA. This association facilitates an almost immediate ability to translate critical ISA information into an INP foiling operation. More broadly, the intimate relationship between the INP and the ISA supports the exchange of intelligence while enabling consistency in both offensive and defensive counterterrorist operations (Hasisi et al., 2009).

Many countries do not have a centralized police system. These countries must coordinate their counterterrorism activities on the national/federal as well as the local levels. In the United States, for example, where there are around 17,000 police organizations on the federal, state, and local levels, there was, before 9/11, a lack of intelligence and operation coordination that has been strongly criticized (Weisburd et al., 2009). Subsequent to 9/11, local, state, and federal law enforcement agencies began to exchange information, as well as to create centralized special officers and units, including special response teams.

Bratton and Kelling (2006) claim that intelligence-led policing is having a strong influence on the major efforts that are being made to restructure police capabilities in the United States for an increasingly proactive intelligence gathering and analysis apparatus. Numerous state and local departments are now creating their own systems, assembling databases and sharing information, rather than relying only upon the federal government for intelligence.

This significant development requires sophisticated coordination, especially in such a large country as the United States, with numerous police organizations. These organizations are applying a set of national strategic guidelines that attempt to define the division of authority and responsibility, setting crucial cooperation and partnership procedures.

Terrorism is a threat not only on the national but also on the international level. Accordingly, collecting and sharing quality intelligence as well as operational cooperation are essential internationally for law enforcement and intelligence organizations in counterterrorism (Kelling & Bratton, 2006). This is especially true due to the connections between terrorist organizations and the classic hardcore criminal organizations, which requires the police to extend the well-established national and international cooperation on fighting organized crime to the foiling of terrorism.

Tenth Commandment—Educate, Communicate, and Update the Public before, during, and after a Terrorist Event

The most important component of counterterrorism is preserving the population's resilience. An important mechanism for achieving this goal involves maintaining the vital communication channels between the police and the public. The police need to wisely educate and update the public before, during, and after a terrorist event.

Before terror attacks, as part of "target hardening," the police should play a central role in preparing and educating the public. The members of the community need to be part of the defensive alignment, as part of a civil guard or by harnessing the citizens' vigilance as part of an early warning system. Even from an early age, the public needs to be made aware of indicators of possible terrorism events, and be trained to report their suspicions to the police. In Israel, for example, police officers teach children in elementary schools to be attentive toward suspicious people and objects, and to notify an adult or, if possible, a police officer. The police in Israel handle every report/call as if it were an actual explosive device or some other security threat, in spite of the fact that the vast majority of security calls to the police are false alarms. By behaving in such a manner, the police display their responsiveness to the public, who are expected to continue calling because of the potential damage from every terrorist attack (Weisburd et al., 2009). Such responsiveness fosters public confidence in the police, who are thus viewed by the public as responding proficiently to emergencies in matters of counterterrorism (Perry, 2014).

Similarly, in the United Kingdom, the police invest a great deal of effort to encouraging public attentiveness to suspicious behavior (suspicious short-term tenants, suspicious people who have bought or rented a car, etc.). The police there strive to develop appropriate reporting mechanisms, alongside establishing working relationships with the private business community to protect businesses from potential threats and to provide guidance on appropriate security measures (Howard, 2004).

An essential element in preserving public resilience during and after a terrorist event is keeping the vital communication channels between the police and the public open in real time. The territorial commander (or deputy or spokesperson) should report calmly and informatively during and after the attack event via the media. Such ongoing communication in real time reduces distress and fear among the public, and these media briefings prevent damaging rumors, giving the public the safe feeling that things are under control. Such debriefings should provide information such as the description of the event, the areas or roads that have been shut down, and alternative routes (Weisburd et al., 2009).

Conclusion

The most effective counterterrorism strategies concentrate on decreasing the opportunities for terrorist attacks, since this is easier than to diminish terrorist motivation. The "Ten Commandments for Effective Counterterrorism" are mostly situational crime prevention techniques not much different from those that law enforcement deploys against "ordinary" criminals (Clarke & Newman, 2006). Many of the methods and resources required to combat terrorism (before, during, or after such an attack) are regularly utilized by the police in their daily routine. These include: investigation, information and evidence collection; forensics (identification of weapons, explosives, victims, etc.); police-operated call centers and first responders; and police liaison with the private sector, including the issuance of licensing to businesses, traffic control, managing crime scenes, and maintaining or restoring public order. Police are responsive to irregularities in the environments in which they operate routinely, and they look out for situational suspicious indicators that also could be connected to terrorism activities in their communities (Innes, 2006). That is one of the main reasons why, in most countries, the police lead the response to terrorism and have a major responsibility for maintaining public security. The connections between terrorists and other criminals put the police in an exceptional position to collect information, giving them an edge in leading the response to terrorism. Criminals facilitate terrorism with many required tools such as weapons and explosives; documentation; vehicles; collecting, transferring, and laundering money; information; communications; and technology. They even issue subcontracts for specific missions. Terrorist organizations, to finance their activities, have used classic organized-crime illegal activities such as money counterfeiting and the smuggling of drugs, counterfeit goods, and taxable merchandise such as cigarettes.

Even though it is not easy to deal with motivation, we accept that, to deal with terrorism, it is advisable to treat both the motivation and the opportunity to commit a terrorist attack. We recognize that one should not belittle the importance of reducing the factors that foster terrorism, yet these are mostly long-term issues and not typically law enforcement missions. They belong to other disciplines such as political science and economics.

However, as noted, such motivations are often embedded in long-term historical grievances that are not likely to be solved in the short term. In the meanwhile, the "Ten Commandments for Counterterrorism" offer solutions for the short term. Situational terror prevention enables an applicable and effective response, though not a perfect answer. Terror attacks encourage radicalization and create a negative atmosphere that prevents political process; therefore, the effort of situational prevention strategies in preventing terror attacks can help create a positive atmosphere for political process, which can help resolve the conflict. Situational crime prevention also helps to divert terror attacks from sensitive targets (e.g., airports and airplanes).

While discussing these counterterrorism strategies, tactics, and practices, one should give some thought to the inherent tension between preserving democratic principles and counterterrorism measures. Liberal values of democratic societies constrain the state's capacity to take full advantage of potential capabilities that the state has in counterterrorism. Since, the "criminal justice model" for counterterrorism views terrorism as a crime and terrorists as violent criminals, terrorists should be arrested and punished according to the rule of law by the police (best qualified to deal with criminals and crime) and the criminal justice system (Greene & Herzog, 2009). Indeed, Perliger, Hasisi, and Pedahzur (2009) claim that there is strong consensus among scholars that the criminal justice model allows responses to terrorism without seriously undermining the legal and moral

foundations of the democratic system. Accordingly, it is better for democratic countries to leave counterterrorism in the hands of the police, which operate in the civilian arena. By contrast, "the war model" (Greene & Herzog, 2009) characterizes terrorism as an act of war that challenges and threatens the well-being of the state and the political system. As such, this model maintains that the terrorist and the terrorist organization should be eliminated by the use of military forces and intelligence. The utilization of this model would involve military forces conducting combat warfare within their own territory, constituting a severe undermining of human rights and morality of the democratic state and its legal system.

The democratic technological state is required to select procedures and utilize capabilities that will cause minimum damage to human rights. The collection and usage of intelligence is part of the "dirty work" of a democracy, according to Innes (2006). Harming individuals not connected to terrorism or harming fundamental moral principles by using superior capabilities would establish a victory for the terrorists. Misuse of such resources will possibly alienate parts of society, playing into the terrorists' hands (Ganor, 2009). This is especially significant in minority communities that are related ethnically or nationally to terrorist groups (Hasisi et al., 2009). In the end, as Bayley and Weisburd (2009) argue, legitimacy is the foundation of successful policing, whether related to terrorism or to regular crime. Losing police legitimacy jeopardizes public cooperation, which is very much needed in counterterrorism. Importantly, the leading role of police in counterterrorism raises new problems and dilemmas for police forces in democratic countries. Counterterrorism puts emphasis on "high policing," which is characterized by its focus on strategic issues at a macro level, rather than local crime and disorder problems (Bayley & Weisburd, 2009; Weisburd et al., 2009). High policing stresses controlling rather than servicing the public, a position very different from the community policing ideas that have reinforced community–police relationships, especially with minorities. It is difficult to be "officer friendly" and at the same time collect intelligence on suspects who are part of or related to the community (Weisburd et al., 2009). In this context, the "Ten Commandments for Counterterrorism" must be adopted in an environment that respects human rights and recognizes the importance of the legitimacy of public evaluations of police strategies.

References

Bayley, D., & Weisburd, D. (2009). Cops and spooks: The role of police in counterterrorism. In D. Weisburd, T. E. Feucht, I. Hakimi, L. F. Mock, & S. Perry (Eds.), *To protect and to serve: policing in an age of terrorism* (pp. 81–99). New York: Springer.

Bratton, W., & Kelling, G. (2006). Policing terrorism. *Civic Bulletin, 43*, 1–10.

Brodeur, J., & Dupeyron, N. (1993). Democracy and secrecy: The French intelligence community. In J. Brodeur, P. Gill, & D. Tollborg (Eds.), *Democracy, law and society* (pp. 19–23). Aldershot: Ashgate.

Clarke, R., & Cornish, B. (2001). Rational choice. In R. Paternoster & R. Bachman (Eds.), *Explaining criminals and crime: Essays in contemporary criminological theory* (pp. 23–42). Los Angeles: Roxbury.

Clarke, R., & Newman, G. (2006). *Outsmarting the terrorists*. Westport, CT: Praeger Security International.

Connors, T. P., & Pellegrini, G. (2005). *Hard won lessons: policing terrorism in the United States*. The Manhattan Institute, New York, Safe Cities Project.

Davis, L. M., Riley, J. K., Ridgeway, G., Pace, J., Cotton, S. K., Steinberg, P. S., ... Smith, B. L. (2004). *When terrorism hits home: how prepared are state and local law enforcement?* Santa Monica: Rand Corporation.

Felson, M., & Clarke, R. (1998). *Opportunity makes the thief: Practical theory for crime prevention.* Police Research Series. Paper 98.

Ganor, B. (2009). Trends in modern international terrorism. In D. Weisburd, T. E. Feucht, I. Hakimi, L. F. Mock, & S. Perry (Eds.), *To protect and to serve: policing in the years of terrorism, and beyond* (pp. 11–42). New York: Springer.

Greene, J. R., & Herzog, S. (2009). The implications of terrorism on the formal and social organization of policing: some concerns and opportunities. In D. Weisburd, T. E. Feucht, I. Hakimi, L. F. Mock, & S. Perry (Eds.), *To protect and to serve: Policing in the years of terrorism, and beyond* (pp. 81–99). New York: Springer.

Hasisi, B., Alpert, G. P., & Flynn, D. (2009). The impacts of policing terrorism on society: Lessons from Israel and the U.S. In D. Weisburd, T. E. Feucht, I. Hakimi, L. Felson Mock, & S. Perry (Eds.), *To protect and to serve: Policing in the years of terrorism, and beyond* (pp. 177–202). New York: Springer.

Howard, P. (Ed.). (2004). *Hard won lessons: How police fight terrorism in the United Kingdom.* New York: Manhattan Institute.

Innes, M. (2006). Policing uncertainty: Countering terror through community intelligence and democratic policing. *Annals of the American Academy of Political and Social Science, 605,* 222–241.

Kelling, G. L., & Bratton, W. J. (2006). Policing terrorism. *Civic Bulletin 43.* New York: Manhattan Institute for Policy Research.

Lum, C., Kennedy, L. W., & Sherley, A. (2006). Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research. *Journal of Experimental Criminology, 2,* 489–516.

Perliger, A., Hasisi, B., & Pedahzur, A. (2009). Policing terrorism in Israel. *Criminal Justice and Behaviour, 36,* 1279–1304.

Perry, S. (2014). Strategies of policing terrorism. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. S5063–S5075). New York: Springer Science+Business Media.

Perry, S., & Hasisi, B. (2015). Rational choice rewards and the Jihadist suicide bomber. *Terrorism and Political Violence, 27*(1), 53–80.

Weisburd, D., & Braga, A. A. (Eds.). (2006). *Police innovation: Contrasting perspectives.* Cambridge, UK: Cambridge University Press.

Weisburd, D., Feucht, T., Hakimi, I., Mock, L., & Perry, S. (2009). Introduction. In *To protect and to serve: policing in the years of terrorism, and beyond* (pp. 1–9). New York: Springer.

Weisburd, D., Jonathan, T., & Perry, S. (2009). The Israeli model for policing terrorism: Goals, strategies, and open questions. *Criminal Justice and Behaviour, 36,* 1259.